

August 18, 2000

INSPECTOR GENERAL INSTRUCTION 7920.5

SUBJECT: Inspector General Small Computer Use

References. See Appendix A.

A. Purpose. This Instruction updates the Office of the Inspector General, Department of Defense (OIG, DoD), Small Computer Use Program.

B. Cancellation. This Instruction supersedes IGDINST 7920.5, *Inspector General Small Computer Use*, August 21, 1997.

C. Applicability

1. This Instruction applies to the Offices of the Inspector General; the Deputy Inspector General; the Assistant Inspectors General; Director, Administration and Information Management; Director, Departmental Inquiries; Director, Intelligence Review; and the Office of the Deputy General Counsel (Inspector General), which is provided support by the OIG. For purposes of this Instruction, these organizations are referred to collectively as OIG components.

2. This Instruction applies to all small computers whether or not they are part of a network.

D. Definitions. See Appendix B.

E. Policy

1. Small computers and the information produced on them shall be protected vigorously from loss, misuse and damage.

2. The OIG, DoD, shall comply with the terms and conditions for commercial software use, including copyright and license agreements.

3. Government office equipment, including small computers, shall only be used for official purposes, except as specifically authorized in this Instruction. Employees are permitted limited appropriate use of Government office equipment for personal needs if the use does not interfere with official business and involves minimal additional expense to the Government. This limited personal use of Government office equipment shall take place during the employee's non-work time. This privilege to use Government office equipment for non-Government purposes may be revoked or limited at any time. This personal use must not result in loss of employee productivity or interference with official duties. Moreover, such use shall incur only minimal additional expense to the Government in areas such as:

- (a) Communications infrastructure costs; e.g., telecommunications traffic, etc.
- (b) Use of consumables in limited amounts; e.g., paper, ink, toner, etc.
- (c) General wear and tear on equipment.

Report Documentation Page		
Report Date 18 Aug 2000	Report Type N/A	Dates Covered (from... to) -
Title and Subtitle Inspector general Small Computer Use	Contract Number	
	Grant Number	
	Program Element Number	
Author(s)	Project Number	
	Task Number	
	Work Unit Number	
Performing Organization Name(s) and Address(es) Inspector General Department of Defense 400 Army Navy Drive Arlington, VA 22202-2884	Performing Organization Report Number	
Sponsoring/Monitoring Agency Name(s) and Address(es)	Sponsor/Monitor's Acronym(s)	
	Sponsor/Monitor's Report Number(s)	
Distribution/Availability Statement Approved for public release, distribution unlimited		
Supplementary Notes		
Abstract		
Subject Terms		
Report Classification unclassified	Classification of this page unclassified	
Classification of Abstract unclassified	Limitation of Abstract UU	
Number of Pages 10		

(d) Data storage on storage devices.

(e) Transmission impacts with moderate electronic mail (E-mail) message sizes, such as E-mails with attachments smaller than 10 megabytes.

3. This policy in no way limits employee use of Government office equipment, including small computers, for official activities.

4. It is the responsibility of employees to ensure that their personal use of Government office equipment is not falsely interpreted to represent the agency. If there is an expectation of such an interpretation, a disclaimer must be used, such as “The contents of this message are mine personally and do not reflect any position of the Government or my agency.”

5. Employees do not have a right, nor should they have an expectation, of privacy while using any Government office equipment at any time, including accessing the Internet or using E-mail. To the extent that employees wish that their private activities remain private, they shall avoid using office equipment such as the computer, Internet or E-mail. By using Government office equipment, employees imply their consent to disclosing the contents of any files or information maintained or passed-through Government office equipment. By using this office equipment, consent to monitoring and recording is implied with or without cause, including (but not limited to) accessing the Internet or using E-mail. Any use of Government small computers is made with the understanding that such use is generally not secure, private or anonymous.

6. The OIG, DoD, reserves the right to monitor all small computer use for the performance of operation, maintenance, auditing, security or investigative functions. Further, monitoring is used to enforce policies regarding official use and harassment and to access information when an employee is not available. The Chief Information Officer (CIO) must provide authorization for this monitoring.

7. Inappropriate personal use of small computers could result in loss of use or limitations on use of the equipment, disciplinary or adverse action, criminal penalties and/or the employee being held financially liable for the cost of the improper use in accordance with reference h.

8. Employees are specifically prohibited from using Government office equipment to maintain or support a personal private business or to assist relatives, friends or other persons in such activities or for personal gain.

9. Access to some OIG, DoD, systems is password-controlled. Access to parts of other OIG, DoD, systems is administratively controlled. Unauthorized access, or attempts to access, controlled systems or areas prohibited or restricted from use, either explicitly or implicitly, is considered misuse of information resources.

10. The use of non-standard hardware or software is a component-level management decision. If the Information Systems Directorate (ISD), Office of Administration and Information Management (OA&IM), determines that non-standard hardware or software are causing a malfunction of standard hardware or software, the ISD reserves the right to return the user to the standard configuration.

11. End users shall not alter configuration of small computers following delivery or repair by the ISD or authorized contractors. Such tampering with hardware (e.g. removal of drives, chips, boards, etc.) may subject the user to administrative penalties in accordance with reference h.

F. Responsibilities

1. The **CIO** shall:
 - a. Approve, for the OIG, DoD, policies implementing laws and guidelines on small computer management.
 - b. Provide leadership to manage small computers within the OIG, DoD.
 - c. Oversee the promulgation of policies and guidance to ensure the most effective, efficient use of small computers.
2. The **ISD** shall:
 - a. Provide CIO-approved hardware, software, telecommunications and other information resources to ensure the efficient, effective use of small computer systems. This includes current anti-virus software.
 - b. Develop small computer policies, standards and procedures.
 - c. Ensure compliance with applicable laws, guidelines, regulations and standards, both internal and external. This includes, but is not limited to, public laws and OIG, DoD, General Services Administration (GSA) and Office of Management and Budget (OMB) publications.
 - d. Manage small computer acquisition, maintenance and support.
 - e. Provide end user support, as defined in the Appendix.
 - f. Administer user identification or authentication mechanisms for those information systems under ISD control.
 - g. Provide advice and assistance to system sponsors for those information systems not under ISD control.
3. The **Personnel and Security Directorate (PSD), OA&IM**, shall:
 - a. Develop small computer security policies, standards and procedures.
 - b. Ensure small computer use complies with applicable security laws, guidelines, regulations and standards, both internal and external. That includes, but is not limited to, public laws and OIG, DoD, Defense Intelligence Agency and OMB publications.
 - c. Perform duties as delegated from the Designated Approving Authority (DAA).
 - d. Advise and assist management on appropriate administrative action(s) if misuse occurs.
4. The **End User** shall:
 - a. Operate small computers within established laws, procedures and guidelines. This includes, but is not limited to, public laws and OIG, DoD, GSA and OMB publications.
 - b. Notify his or her supervisor and the ISD of every occurrence of loss, significant misuse or significant damage to small computers and their contents.

IGDINST 7920.5

- c. Ensure the accuracy and integrity of data input, processed and transmitted.
- d. Refrain from any inappropriate personal uses.
- e. Refrain from tampering with or modifying hardware following delivery or repair of any small computers by the ISD or authorized contractors if this alters the configuration.

5. **Supervisors** shall:

- a. Monitor all small computer use of their employees and take every reasonable step to minimize waste and prevent misuse of the resources.
- b. Designate responsible custodians for all components of information systems in their physical areas.
- c. Develop procedures to ensure the effective, secure operation of information systems in their mission areas, to include ensuring that:
 - (1) All users protect information and information resources;
 - (2) All software used in his or her area is properly inventoried.
 - (3) All reasonable steps are taken to prevent infection of systems with viruses.
 - (4) All users refrain from any tampering or modifying hardware following delivery or repair by the ISD or authorized contractors.
 - (5) All users make only authorized use of systems.
 - (6) All software licensing agreements are enforced.
- d. Communicate to all employees their decisions regarding the authorized uses of communication systems and non-standard software and hardware.
- e. Initiate or take appropriate disciplinary action against employees who violate this Instruction, in accordance with reference h as appropriate.

G. Procedures

1. **Protection of Information.** Since the information stored in, and processed by, small computers frequently is more valuable than the computer itself, users must take steps to preserve its integrity and protect it from infection by viruses. References d and f provide additional precautions.

- a. Storage media must be protected and labeled commensurate with the sensitivity or classification level of the information to which they have been exposed. This includes proprietary information, information subject to the Privacy Act or other unclassified but sensitive information. Data deletion commands do not purge storage media of data. Although the user has deleted the file name, the data may still be accessible. As a minimum, if diskettes have ever been exposed to sensitive data, they shall be placed out of sight, to avoid viewing of or tampering with data.
- b. The user shall position information resources away from windows, open doorways and other viewing areas to discourage theft and prevent disclosure of data to unauthorized persons.

c. Users shall duplicate or back up mission-critical information and files that have taken significant time to create, and store them separately from the original.

d. If the end user introduces any hardware or software into the OIG, DoD, environment that the ISD did not issue, the user is responsible for it. This includes any effect that it may have on the operation of standard hardware and software, as defined in reference e. Even virus-free information resources may cause conflicts. If the ISD determines that non-standard hardware or software is causing a malfunction of standard hardware or software, the ISD reserves the right to return the user to the standard configuration. The ISD shall not assume responsibility for any functionality or data lost by return to the standard configuration.

e. Users of electronic bulletin boards or the Internet shall exercise caution. Many computer viruses are spread through such entryways. There is significant risk in downloading or using programs from electronic bulletin boards and the Internet.

f. No user shall attempt to make unauthorized uses of resources. That includes, but is not limited to, connecting to a system, or part of a system, to which access is unauthorized. Parts of systems are administratively controlled to protect the integrity of systems and agency operations.

g. No user shall process classified information on a small computer that the DAA has not accredited for that level.

2. Licensing Agreements

a. Manufacturers set licensing agreements, and they differ somewhat on the OIG, DoD, software packages specified in reference e. All agreements prohibit copying of printed materials, lending the software or making more than one copy of media.

b. All users are responsible for abiding by the terms of licensing agreements. The ISD has copies of software licensing agreements on large buys. On smaller buys, the agreements accompany distributed software.

c. No software purchased by the OIG, DoD, may be used on-site or off-site apart from accompanying OIG, DoD, owned hardware, unless specifically allowed in the licensing agreement in force at the time the software was purchased. Manufacturers revise licensing agreements at various times even on the same version of the same software. The prohibition generally includes, but is not limited to, the use of OIG, DoD, software on privately owned equipment, even if it is being used for work-related tasks. The restriction is necessary to conform with the prohibitions in most software licensing agreements against lending software or making it available to others. Utility programs used to retrieve information in the course of an investigation or audit are exempted from this restriction. However, users of such programs must ensure that they vigorously avoid infecting systems or violating software licensing agreements.

3. Operational Security

a. Moving or disconnecting small computers may affect network operations or the security of a previously accredited configuration that processes classified material. Therefore, if a small computer is part of a network or accredited configuration, the user shall request support, as specified in reference g, to move or disconnect the computer.

b. Users must take all reasonable precautions to physically secure information resources. The precautions apply to on-site use, as well as transporting or using the resources off-site. For example, resources are in jeopardy if left unattended in plain view in an unlocked hotel room

while in travel status or in the passenger compartment of an automobile. The user shall take the same precautions he or she would take to protect valuable personal property, such as a camera.

c. Whoever is charged within the component with password management must protect passwords and make sure they are changed frequently.

d. Users shall appropriately label all media containing sensitive and classified information.

e. Before using an accredited system, users shall read and understand applicable operational procedures.

4. Accountability

a. Beverage and all other liquid containers shall never be placed near computers. If spilled, they shall cause extensive damage to the computer or its elements.

b. Storage media require special care. Temperature extremes, dampness, fingerprints, dust, spilled liquids, cigarette smoke, eraser dust and pressure may damage the recording surface. To protect media from accidental damage, users must ensure the media are protected according to manufacture's instructions.


c. All provisions of reference i shall be followed.

d. End users shall not tamper with or modify hardware following delivery or repair of any small computers by the ISD or authorized contractors. This includes removing drives, chips, boards, etc.

e. The ISD has a limited number of small computers and the software and peripherals necessary for approved off-site tasks. They may be signed out by OIG, DoD, employees or contractors for a length of time to be determined by the ISD based on availability and demand. The approval must be authorized in writing. If the requester is an OIG, DoD, contractor, his or her Contracting Officer's Technical Representative must approve the request. If the requester is an OIG, DoD, employee, his or her supervisor must approve.

H. Effective Date and Implementation. This Instruction is effective immediately.

FOR THE INSPECTOR GENERAL:


Joel L. Leson
Director
Office of Administration
and Information Management

2 APPENDICES - A/S

APPENDIX A REFERENCES

- a. DoD Directive 8000.1, "Defense Information Management (IM) Program," October 27, 1992.
- b. DoD Instruction 5500.7, "Standards of Conduct," August 30, 1993.
- c. DoD Regulation 5500.7-R, "Joint Ethics Regulation (JER)," August 1993, as changed.
- d. IGDM 5200.1, *Information Security Program*, August 1, 1988, as changed.
- e. IGDINST 7950.2, *Inspector General Microcomputer Hardware and Software Management Program*, May 23, 2000.
- f. IGDINST 7950.4, *Microcomputer Antiviral Initiative*, February 26, 1992.
- g. IGDINST 8000.2, *Request for Information Services Directorate (ISD) Services*, September 15, 1998.
- h. IGDR 1400.4, *Disciplinary and Adverse Action*, December 30, 1994.
- i. IGDM 7200.10, *Accountable Property Management Program*, September 30, 1994, with Change.

This page left blank intentionally

APPENDIX B DEFINITIONS

- a. **Accredited configuration** is hardware, firmware, software, procedures and documentation that have been formally declared by the Designated Approving Authority as approved to operate at a designated security level using a prescribed set of safeguards.
- b. **Chief Information Officer (CIO)** is the senior official, appointed by the Inspector General, who is responsible for developing and implementing information resources management in ways that enhance OIG, DoD, mission performance through the effective, economic acquisition and use of information. The CIO is currently the Director of the Office of Administration and Information Management.
- c. **Communication systems** include Government-owned telephones, facsimile machines, electronic mail, Internet systems and commercial systems when use is paid for by the Federal Government.
- d. **End user** is an OIG, DoD employee or contractor who uses automated equipment to perform work-related tasks.
- e. **End user support** includes diagnosing and resolving problems about operating and using standard OIG, DoD hardware, software, telecommunications and software applications.
- f. **Designated Approving Authority (DAA)** is the official, appointed by the Inspector General, who has the authority to decide on accepting the security safeguards prescribed for an information system or that official who may be responsible for issuing an accreditation statement that records the decision to accept these standards. The DAA is currently the Director of the Office of Administration and Information Management.
- g. **Employee non-work time.** Times when the employee is not otherwise expected to be addressing official business. Employees may, for example, use Government office equipment during off-duty hours, such as before or after a workday (subject to local office hours), lunch periods, authorized breaks or weekends or holidays (if the employee's duty station is normally available at such times).
- h. **Inappropriate personal uses.** Employees are expected to conduct themselves professionally in the workplace and to refrain from using Government office equipment for activities that are inappropriate. Misuse or inappropriate personal use of Government office equipment includes, but is not limited to:
 - 1. Any personal use that could cause congestion, delay or disruption of service to any Government system or equipment.
 - 2. Using the Government systems as a staging ground or platform to gain unauthorized access to other systems.
 - 3. Using Government office equipment for activities that are illegal, inappropriate or offensive to fellow employees or the public. Such activities include, but are not limited to, hate speech or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin or sexual orientation.
 - 4. The creation, downloading, viewing, storage, copying or transmission of sexually explicit or sexually oriented materials.

5. The creation, downloading, viewing, storage, copying or transmission of materials related to gambling, weapons, terrorist activities and any other illegal activities or activities otherwise prohibited, etc.
 6. Use for commercial purposes or in support of "for-profit" activities or in support of other outside employment or business activity (e.g., consulting for pay, sales or administration of business transactions, sale of goods or services) or for personal gain.
 7. Engaging in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity or engaging in any prohibited partisan political activity.
 8. Any use that could generate more than minimal additional expense to the Government.
 9. The unauthorized acquisition, use, reproduction, transmission or distribution of any controlled information, including computer software and data that includes privacy information, copyrighted, trade marked or material with other intellectual property rights (beyond fair use), proprietary data or export controlled software or data.
- i. **Information** is any communication or reception of knowledge, such as facts, data or opinions, including numerical, graphic or narrative forms, maintained in any medium, including but not limited to, computerized data bases, paper, microform or magnetic tape.
 - j. **Information resources** are any combination of hardware, software and telecommunications, along with documentation and automated and manual procedures, that provide the information necessary to accomplish organizational missions and objectives.
 - k. **Information system** is the organized collection, processing, transmission and dissemination of information according to defined procedures, whether automated or manual. It includes people, equipment and policies.
 - l. **Sensitive but unclassified information** is any information that has not been specifically authorized to be kept classified, but that if lost, misused, disclosed or destroyed, could adversely affect the national interest or the conduct of OIG, DoD, operations or Federal programs, or the privacy to which individuals are entitled under the Privacy Act. Typical types of data considered sensitive are "For Official Use Only," proprietary, financial and mission-critical information.
 - m. **Small computers** are computers that have self-contained processing units and are easily transportable. The definition includes, but is not limited to, personal computers, programmable calculators and desktop, laptop, palmtop and notebook computers.
 - n. **Storage media** include, but are not limited to, hard disks, floppy disks, optical disks, compact disks and magnetic tapes.
 - o. **System** is a collection of people, equipment, policies and methods organized to accomplish an activity.
 - p. **Virus**, as used in this Instruction, includes all malicious software. Those malicious programs may be viruses, worms, Trojan horses or bombs.